National Cybersecurity and Communications Integration Center

BULLETIN **201204301400**

Court Order Aiding Computers Infected with DNSChanger Malware Set to Expire

Executive Overview

(U) In November 2011, a group of six Estonians and one Russian were charged with creating/operating the DNSChanger malware used to engage in wire fraud. The malware may have prevented users' anti-virus software from working correctly allowing the malware to take control of the computer's domain name system (DNS). DNSChanger malware enabled internet requests to be forwarded to rogue servers instead of legitimate ones.

(U) The FBI obtained a court order that allowed millions of computers connected to the rogue DNS servers to instead connect to clean servers allowing the infected computers to resolve domain names correctly. However, the court order aiding computers infected with the DNSChanger will expire July 2012.

(U) The initial court order has safely, but temporarily, disabled DNSChanger's ability to redirect infected computers. It is possible that a user has an infected computer, but is unaware of the DNSChanger infection. Resources are available for users to examine if they are infected with the DNSChanger malware. Identifying an infection and cleaning the malware from the computer will prevent loss of Internet access.

Background

(U) The court order which expires in July authorizes the creation of clean servers, which are operated by the Internet Systems Consortium for infected computers to utilize. When the order expires, computers routed through the clean, temporary servers will lose the ability to resolve domain names, which would severely impact their ability to connect to the Internet.

(U) Both the US-CERT and FBI have previously documented DNSChanger

- February 23, 2012, US-CERT summary on DNSChanger Malware: http://www.us-cert.gov/current/#operation_ghost_click_malware

- November 2011 FBI document detailing DNS settings and the DNSChanger malware: http://www.fbi.gov/news/stories/2011/november/malware_110911/dns-changer-malware.pdf

(U) For further information regarding the court case (United States v. Vladimir Tsastsin, et. al, 11 Cr. 878.), please visit the US Attorney's Office, Southern District of New York website: http://www.justice.gov/usao/nys/vladimirtsastsin.html

Mitigation

(U) Users should take the following steps to clean their computers infected with the DNSChanger:

1. (U) **Home Users**: Check to see if you are affected by visiting the following DNSChanger Test Site:
    - www.dns-ok.us
2. (U) If you are not affected by DNSChanger, then no further action is required.
3. (U) If the site indicates that you are affected, visit www.dcwg.org for information on how to address this problem. After following the clean-up advice, check back with one of the Test sites above.
4. (U) **Internet Service Providers (ISPs), Businesses and other Large Organizations**: To determine if your organization and user base are relying on the DNSChanger Clean DNS Servers, check for traffic leaving your network destined for any of the following IP addresses:
    - 85.255.112.0 through 85.255.127.255
    - 67.210.0.0 through 67.210.15.255
    - 93.188.160.0 through 93.188.167.255
    - 77.67.83.0 through 77.67.83.255
    - 213.109.64.0 through 213.109.79.255
    - 64.28.176.0 through 64.28.191.255

    Traffic destined for these IP addresses may indicate DNSChanger or other malware infections.

(U) The aforementioned methods are the best way to determine if computers on your network are relying on the DNSChanger Clean DNS Servers. If you are not able to accomplish egress filtering or otherwise monitor traffic leaving your network then please visit http://dcwg.org/cleanup.html for a list of organizations that may be able to provide data on affected IP addresses within your network.

Points of Contact

(U) Please direct questions to the NCCIC Duty Officer (NDO) via email at NCCIC@hq.dhs.gov or by phone at (703) 235-8831. The NCCIC will continue to coordinate with the appropriate component organizations.